

Web Images Videos Maps News Shopping Gmail more ▾

[Sign in](#)

Google scholar

"public key" broadcast (mobile OR radio)

Search

[Advanced Scholar Search](#)
[Scholar Preferences](#)

- ☒ Search only in Engineering, Computer Science, and Mathematics.
☐ Search in all subject areas.

Scholar

Articles and patents

- 2003

include citations

Results 1 - 100 of abc

[PDF] Secure link state routing for **mobile** ad hoc networks

P Papadimitratos, ZJ Haas - IEEE Workshop on Security and Assurance ..., 2003 - Citeseer

... Clearly, SLSP nodes should be able to perform **public key** operations. ... First, nodes reduce or increase their LSU **broadcast** period according to the network conditions. ... 4. Conclusions and future work We proposed a secure link state protocol (SLSP) for **mobile** ad hoc networks. ...

[Cited by 159](#) - [Related articles](#) - [View as HTML](#) - [All 16 versions](#)

[PDF] Secure routing for **mobile** ad hoc networks

P Papadimitratos, ZJ Haas - SCS Communication Networks and ..., 2002 - Citeseer

... Abstract The emergence of the **Mobile** Ad Hoc Networking (MANET) technology advocates self-organized ... could be instantiated, for example, by the knowledge of the **public key** of the ... Finally, the **broadcast** nature of the **radio** channel mandates that each transmission is received ...

[Cited by 957](#) - [Related articles](#) - [View as HTML](#) - [All 51 versions](#)

... anonymous on demand routing with untraceable routes for **mobile** ad-hoc networks

J Kong, X Hong - ... of the 4th ACM international symposium on **Mobile** ..., 2003 - portal.acm.org

... The first one is a naive porting of MIX-Net to **mobile** ad hoc networks. ... Compared to ANODR-PO, ANODR-BO ensures that no **public key** operation is executed during RREQ ... 3 shows the case where anonymous route discovery depends completely on local **broadcast** with trap ...

[Cited by 291](#) - [Related articles](#) - [All 27 versions](#)

Security and privacy aspects of low-cost **radio** frequency identification systems

S Weis, S Sarma, R Rivest, D Engels - Security in Pervasive Computing, 2003 - Springer

... This is far below what is feasible for standard **public-key** or symmetric encryption, including efficient ... Security and Privacy Aspects of Low-Cost **Radio** Frequency Identification Systems ... We present a variant of binary tree walking which does not **broadcast** insecure tag IDs on the ...

[Cited by 776](#) - [Related articles](#) - [BL Direct](#) - [All 26 versions](#)

[CITATION] Secure **broadcasting** using the secure lock

GH Chiou, WT Chen - IEEE Transactions on Software Engineering, 1989

[Cited by 198](#) - [Related articles](#) - [All 10 versions](#)

[CITATION] Pre-loaded key based multicast and **broadcast** authentication in **mobile** ...

M Ramkumar, N Menon - IEEE Global Telecommunications Conference, 2003. ..., 2003

[Cited by 32](#) - [Related articles](#) - [All 7 versions](#)

[PDF] The TESLA **broadcast** authentication protocol

A Perrig, R Canetti, JD Tygar, D Song - RSA CryptoBytes, 2002 - Citeseer

... Examples of **broadcast** distribution networks are satellite broadcasts, wireless **radio broadcast**, or IP multicast. ... TESLA is used in a wide variety of applications, ranging from **broadcast** authentication in sensor ... signature key pair, with the private key K^{-1}_S and the **public key** K_S ...

[Cited by 389](#) - [Related articles](#) - [View as HTML](#) - [All 29 versions](#)

Mobile wireless computing: challenges in data management

T Imielinski, BR Badrinath - Communications of the ACM, 1994 - portal.acm.org
 ... What is the role of a wireless medium in distribution of information? How can one query data that is **broadcast** over the wireless? ... These are special **mobile radio** networks provided by private service providers such as RAM and ARDIS. ...
[Cited by 582](#) - [Related articles](#) - [BL Direct](#) - [All 6 versions](#)

[PDF] Secret key agreement by public discussion from common information

UM Maurer... - IEEE Transactions on Information Theory, 1993 - Citeseer
 ... For instance the security of the well-known RSA **public-key** cryptosystem [1] is based on the (unproven) difficulty of factoring large integers, and many ... This **broadcast** channel scenario is generalized in Section 3 to a scenario where Alice, Bob and Eve know random variables ...
[Cited by 522](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 27 versions](#)

Proactive **public key** and signature systems

A Herzberg, M Jakobsson, S Jarecki, H ... - Proceedings of the ..., 1997 - portal.acm.org
 ... work deals with the general theory of proactive memory maintenance and computation in the presence of **mobile** faults in ... (Note that, here we assume **broadcast**. ... the model of [HJKY], where proactive secret sharing was introduced and we adopt it to proactive **public key** systems. ...
[Cited by 213](#) - [Related articles](#) - [All 11 versions](#)

Route optimization for **mobile** IP

CE Perkins, DB Johnson - Cluster Computing, 1998 - Springer
 ... Finally, this notification allows any resources consumed by the **mobile** node at the previous foreign agent (such as an allocated **radio** channel) to be released immediately, rather than waiting for its registration lifetime to expire. ...
[Cited by 574](#) - [Related articles](#) - [BL Direct](#) - [All 5 versions](#)

[PDF] Providing robust and ubiquitous security support for **mobile** ad-hoc networks

H Luo, J Kong, P Zerfor, S Lu, L Zhang - IEEE ICNP, 2001 - Citeseer
 ... n may be dynamically changing as **mobile** nodes join, leave, or fail over time. ... (1) The **public key** PK for ... than in their wired counterpart [34], monitoring and detecting misbehaviors among one-hop neighbors are readily easier and more practical due to the **broadcast** nature of ...
[Cited by 541](#) - [Related articles](#) - [View as HTML](#) - [All 29 versions](#)

[PDF] Random key predistribution schemes for sensor networks

H Chan, A Perrig, D Song - IEEE Symposium on Security and Privacy, 2003 - Citeseer
 ... The ISM band **radio** receiver communicates at a peak rate of 40Kbps at a range of up to ... and power resources of sensor nodes often makes it undesirable to use **public-key** algorithms, such ... This can be accomplished with a simple local **broadcast** of all key identifiers that a node ...
[Cited by 1504](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 53 versions](#)

A quick group key distribution scheme with "entity revocation"

J Anzai, N Matsuzaki, T Matsumoto - Advances in Cryptology- ..., 1999 - Springer
 ... concept and a concrete scheme of a conference key distribution for secure digital **mobile** communications with ... in section 3. Moreover, we consider that a time-stamp on the **broadcast** data is ... To prevent an attacker from modifying and forging a **public key** on a public bulletin board ...
[Cited by 74](#) - [Related articles](#) - [BL Direct](#) - [All 3 versions](#)

[PDF] An authentication and security protocol for **mobile** computing

Y Zheng - IFIP World Conference on Mobile Communications, 1996 - Citeseer
 ... This section proposes an authentication and key distribution protocol based on a **broadcast** channel in a ... involves a trusted certification authority ca which provides participants of the network, including **mobile** users and base stations, with **public key** certification services. ...
[Cited by 37](#) - [Related articles](#) - [View as HTML](#) - [All 4 versions](#)

Environmental key generation towards clueless agents

J Riordan, B Schneier - **Mobile Agents and Security**, 1998 - Springer

... Unfortunately these techniques are not applicable to **mobile** agents due to the fact that software, unlike hardware, is completely and trivially ... 2. The server returns the **public key**, D , for that time. ... 5. The server returns E_i . (Again, the server could continuously **broadcast** E_i). ...

Cited by 176 - Related articles - BL Direct - All 15 versions

[PDF] HiperLAN/2--The broadband **radio** transmission technology operating in the ...

M Johnsson - HiperLAN/2 Global Forum, 1999 - Citeseer

... are bidirectional whereas point-to-multipoint are unidirectional in the direction towards the **Mobile Terminal** ... **Broadcast** and multicast traffic can also be protected by encryption through the use of common keys (all ... one is to use a pre-shared key and the other is to use a **public key**. ...

Cited by 93 - Related articles - View as HTML - All 27 versions

[CITATION] Cryptology for digital TV **broadcasting**

BM Macq, JJ Quisquater - Proceedings of the IEEE, 1995

Cited by 305 - Related articles - BL Direct - All 4 versions

[PDF] Security in public **mobile** communication networks

H Federrath, A Jerichow, D Kesdogan, A ... - WISSENSCHAFTLICHE ..., 1995 - Citeseer

... completely anonymous to the network by delivering the message (possibly end-to-end-encrypted) to all stations (**broadcast**). ... Change of encoding of a message can be implemented using a **public-key** cryptosystem. ... 2.2.1 **Mobile Radio** Systems with Reduced Locating-Ability ...

Cited by 30 - Related articles - View as HTML - BL Direct - All 17 versions

MIXes in **mobile** communication systems: Location management with privacy

H Federrath, A Jerichow, A Pfitzmann - Information Hiding, 1996 - Springer

... The attacker could simply encrypt the outgoing messages of a MIX M_i using its **public key** CM_i and ... of the next register (AR1) which, in turn, stores the location information of the **mobile** subscriber. ... P2 to store the LAI and the implicit address TMSI for the **broadcast** message on ...

Cited by 58 - Related articles - BL Direct - All 25 versions

[PDF] Key management for large dynamic groups: One-way function trees and ...

D Balenson, D McGrew, A Sherman - 1999 - securitytechnet.com

... be able to take advantage of efficient **broadcast** channels, such as **radio broadcast** and Internet ... published methods, our algorithm achieves a new low in the required **broadcast** size. ... distributed functionality, they suffer from a linear number of expensive **public-key** operations. ...

Cited by 218 - Related articles - View as HTML - All 12 versions

[PDF] Key establishment in large dynamic groups using one-way function trees

DA McGrew, AT Sherman - Manuscript submitted to IEEE Transactions on ..., 1998 - Citeseer

... be able to take advantage of efficient **broadcast** channels, such as **radio broadcast** and Internet ... linear number of **public-key** operations, which are slow in software relative to encryption ... The LKH method [14, 15] achieves logarithmic **broadcast** size, storage, and computational cost. ...

Cited by 279 - Related articles - View as HTML - All 11 versions

[CITATION] Toward secure key distribution in truly ad-hoc networks

A Khalili, J Katz, WA Arbaugh - Applications and the Internet Workshops, 2003. ..., 2003

Cited by 221 - Related articles - All 14 versions

[CITATION] Preserving privacy in a network of **mobile** computers

DA Cooper, KP Birman - 1995 IEEE Symposium on Security and Privacy, 1995. ..., 1995

Cited by 88 - Related articles - BL Direct - All 23 versions

Networks without user observability—design options

A Pfitzmann, M Waidner - Advances in Cryptology—EUROCRYPT'85, 1985 - Springer

... for the classical **broadcast** services TV and **radio**, great parts of the life of any user could ... message can be made completely anonymous to the network by delivering the message to all stations (**broadcast**). ... Invisible implicit addresses can be realized with a **public key** cryptosystem ...

[Cited by 220](#) - [Related articles](#) - [All 8 versions](#)

A key-management scheme for distributed sensor networks

L Eschenauer, VD Gligor - Proceedings of the 9th ACM Conference ..., 2002 - portal.acm.org

... of the network, and control nodes, which monitor the status of and **broadcast** simple commands ... have limited, if any, mobility after deployment, some nodes are highly **mobile** (eg, data ... nodes in this range make it impractical to use typical asymmetric (**public-key**) cryptosystems to ...

[Cited by 1814](#) - [Related articles](#) - [All 55 versions](#)

Key-insulated **public key** cryptosystems

Y Dodis, J Katz, S Xu, M Yung - Advances in Cryptology—EUROCRYPT ..., 2002 - Springer

... Cryptographic computations (decryption, signature genera- tion, etc.) are often performed on a relatively insecure device (eg, a **mobile** device or an Internet-connected ... All cryptographic computations are still done on the insecure device, and the **public key** remains unchanged. ...

[Cited by 186](#) - [Related articles](#) - [BL Direct](#) - [All 17 versions](#)

[CITATION] The first ten years of **public-key** cryptography

W Diffie, BN Res, M View - Proceedings of the IEEE, 1988

[Cited by 220](#) - [Related articles](#) - [All 13 versions](#)

[PDF] **Public key** protocols for wireless communications

C Boyd, DG Park - Proceedings of the 1st International Conference on ..., 1998 - Citeseer

... As for A's way to get the **public key** of the network, it may receive the key value from the system **broadcast** channel of ... B can get the **public key** of the user from the certificate data of A if it is included inside the ... Note that the first message can be pre-calculated off-line by the **mobile**. ...

[Cited by 40](#) - [Related articles](#) - [View as HTML](#) - [All 10 versions](#)

[PDF] Design issues in **mobile-agent** programming systems

NM Karnik, AR Tripathi - IEEE concurrency, 1998 - Citeseer

... be integrated with the name resolution service, so that a name lookup can return a **public key** in addition ... Table 2 summarizes the basic mobility support provided by the seven **mobile** agent systems surveyed ... Another model is to provide **broadcast** of events to all agents in a group ...

[Cited by 278](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 13 versions](#)

[CITATION] **Mobile** networking through **mobile** IP

CE Perkins, S Microsyst, M View - IEEE Internet computing, 1998

[Cited by 906](#) - [Related articles](#) - [BL Direct](#) - [All 59 versions](#)

[PDF] ... of key chain commitments for **broadcast** authentication in distributed sensor ...

D Liu, P Ning... - Proceedings of the 10th Annual Network and ..., 2003 - Citeseer

... networks. Gen- erally, an asymmetric mechanism, such as **public key** cryptography, is required to authenticate **broadcast** messages. Otherwise, a malicious receiver can easily forge any packet from the sender. However, due to the ...

[Cited by 166](#) - [Related articles](#) - [View as HTML](#) - [All 20 versions](#)

[PDF] A novel authentication scheme for ad hoc networks

L Venkatraman, DP Agrawal - IEEE Wireless Communications and ..., 2000 - Citeseer

... purview. The CA ought to be a completely trusted entity and issues a digi- tal certificate to any **mobile** host that needs to be authen- ticated. ... members. This key is encrypted with the system **public key** and **broadcast** by the head. Each ...

[Cited by 77](#) - [Related articles](#) - [View as HTML](#) - [All 9 versions](#)

SEAD: Secure efficient distance vector routing for **mobile** wireless ad hoc networks

YC Hu, DB Johnson, A Perrig - Ad Hoc Networks, 2003 - Elsevier

... that can create routing loops are more common in wireless and **mobile** networks such ... trust relationships from PGP-like certificates without relying on a trusted **public key** infrastructure [19]. ... Any efficient **broadcast** authentication mechanism, such as TESLA [37], HORS [42], or TIK ...

[Cited by 775](#) - [Related articles](#) - [All 53 versions](#)

Mitigating routing misbehavior in **mobile** ad hoc networks

S Marti, TJ Giuli, K Lai, M Baker - ... international conference on Mobile ..., 2000 - portal.acm.org

... One advantage of wireless is the ability to transmit data among users in a common area while remaining **mobile**. ... not have this information (for instance if it were implemented on top of a hop-by-hop routing protocol), then a malicious or broken node could **broadcast** the packet to ...

[Cited by 1692](#) - [Related articles](#) - [All 74 versions](#)

Proxy-based security protocols in networked **mobile** devices

M Burnside, D Clarke, T Mills, A Maywah, S ... - Proceedings of the ..., 2002 - portal.acm.org

... Devices themselves may be **mobile** and may change loca- tions. ... At the same time that this information is **broadcast** in the I-F spectrum, the beacon also ... 4. PROXY TO PROXY PROTOCOL SPKI/SDSI (Simple **Public Key** Infrastructure/Simple Dis- tributed Security Infrastructure) [7 ...

[Cited by 67](#) - [Related articles](#) - [All 29 versions](#)

Authenticated ad hoc routing at the link layer for **mobile** systems

J Binkley, W Trost - Wireless Networks, 2001 - Springer

... In the ad hoc protocol, all communicants **broadcast** beacons, not just **Mobile**-IP agents. ... registration packet could include the authenticated addressing information and the **mobile** node would ... The symmetric keys might be replaced with **public key** cryptography [6]. Portland State ...

[Cited by 51](#) - [Related articles](#) - [BL Direct](#) - [All 22 versions](#)

Multicast security and its extension to a **mobile** environment

L Gong, N Shacham - Wireless Networks, 1995 - Springer

... We also describe an initial architectural design for secure multicast in a **mobile** environment. We conclude 9 JC Baltzer AG, Science Publishers ... the order of $O(2n)$. The problem we examine here is how to securely **broadcast** a message when **public-key** sys- tems are ...

[Cited by 53](#) - [Related articles](#) - [All 8 versions](#)

[PDF] Location management strategies increasing privacy in **mobile** ...

D Kesdogan, H Federrath, A Jerichow, A ... - 12th International ..., 1996 - Citeseer

... For the reachability of a **mobile** subscriber signaling takes place in more than one LA. ... Another difference to GSM is the necessary bandwidth on the **broadcast** channel for signaling. By using **public key** cryptography, one paging message is approximately 500 bit long. ...

[Cited by 28](#) - [Related articles](#) - [View as HTML](#) - [All 23 versions](#)

Methods and apparatus for providing a secure paging system

EH Frank, DC Jackson - US Patent 5,285,496, 1994 - Google Patents

... **Radio** paging systems are widely utilized in today's in addition, it is preferred that a secure paging system **mobile** environment. ... a message M to Although there is no way to prevent the pager mes- another user B and A knows B's **public key**, user A can sages **broadcast** on the ...

[Cited by 22](#) - [Related articles](#) - [All 2 versions](#)

[PDF] MOCA: **Mobile** certificate authority for wireless ad hoc networks

S Yi, R Kravets - 2nd Annual PKI Research Workshop Pre-Proceedings, 2003 - Citeseer

... PKI (**Public Key** Infrastructure), an infrastructure for managing digital certificates, was introduced exactly for ... operator chooses MOCAs based on an observation of heterogeneity among **mobile**

nodes, typically ... a certification service cheaply by using a one-hop **broadcast** for the ...

[Cited by 200](#) - [Related articles](#) - [View as HTML](#) - [All 29 versions](#)

SPINS: Security protocols for sensor networks

A Perrig, R Szewczyk, JD Tygar, V Wen, DE Culler - *Wireless networks*, 2002 - Springer

... Keywords: secure communication protocols, sensor networks, **mobile** ad hoc networks, MANET ... and developing μ TESLA (the "micro" version of TESLA), providing authenticated streaming **broadcast**. ... bytes RAM 512 bytes EEPROM Communication 916 MHz **radio** Bandwidth 10 ...

[Cited by 2052](#) - [Related articles](#) - [BL Direct](#) - [All 163 versions](#)

Business models and transactions in **mobile** electronic commerce: requirements ...

A Tsaigatidou, E Pitoura - *Computer Networks*, 2001 - Elsevier

... If used, eg, to **broadcast** multimedia contents over the network, the network would collapse, because ... is charged per connection-time, while for others (eg, in packet **radio**), it is ... of tariffs, eg, session-based, transaction-based, connection time-based, while in **mobile** e-commerce ...

[Cited by 126](#) - [Related articles](#) - [All 15 versions](#)

[CITATION] A streaming architecture for next generation internet

A Dutta, H Schulzrinne, T Technol, NJ Morristown - *IEEE International Conference ...*, 2001

[Cited by 21](#) - [Related articles](#) - [All 9 versions](#)

[CITATION] Techniques for privacy and authentication in personal ...

D Brown - *IEEE [see also IEEE Wireless Communications]* ..., 1995

[Cited by 77](#) - [Related articles](#) - [All 6 versions](#)

Method and apparatus for encrypting **radio** traffic in a telecommunications network

J Rune - *US Patent 5,850,444*, 1998 - *Google Patents*

... FIG. 4 also illustrates a method that can be used to encrypt **radio** communications between a generic access network and a **mobile** terminal, in accordance with another embodiment of the present invention. ... The RNC can **broadcast** the **public key** in all cells in the RNC's ...

[Cited by 18](#) - [Related articles](#) - [All 5 versions](#)

[CITATION] Securing ad hoc networks

L Zhou, ZJ Haas - *IEEE network*, 1999

[Cited by 1764](#) - [Related articles](#) - [BL Direct](#) - [All 88 versions](#)

Identity-based conference key distribution systems

K Koyama, K Ohta - *Advances in Cryptology—CRYPTO'87*, 1987 - Springer

... and Fiat proposed identity-based signature schemes [1, 21, and Okamoto proposed an identity-based scheme [3] for a **public key** distribution system [4 ... If a conference is carried out in **radio-broadcast** networks, this attack would be detectable by the encryption-and-decryption test ...

[Cited by 66](#) - [Related articles](#) - [All 6 versions](#)

[PDF] Challenges in **mobile** electronic commerce

A Tsaigatidou, J Veijalainen, E Pitoura - *Proc. of 3rd International ...*, 2000 - Citeseer

... **Broadcasting** offers an efficient means to disseminate information to a large consumer population. ... For example, if a customer buys a product through its **mobile** phone, this ... Techniques like the asymmetric cryptographic algorithm (also called **Public Key** algorithm) are used to ...

[Cited by 49](#) - [Related articles](#) - [View as HTML](#) - [All 9 versions](#)

... of the asymmetric cryptography in GSM, GPRS, UMTS, and its **public key** ...

CF Grecas, SI Maniatis, IS Venieris - *Mobile Networks and Applications*, 2003 - Springer

... entire network facilitates as well the distribution of the public key in the case of **mobile** network interconnections ... sends the Identity Message to the MSC/VLR with its identity data, using the VLR's **public key**, see figure 3, possibly emitted on the **Broadcast** Channel (BCH ...

[Cited by 26](#) - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)

[CITATION] ... on "Dynamic participation in a secure conferencescheme for **mobile** ...

SL Ng - IEEE Transactions on Vehicular Technology, 2001

[Cited by 16](#) - [Related articles](#) - [BL Direct](#) - [All 3 versions](#)

[CITATION] A new set of passive routing attacks in **mobile** ad hoc networks

J Kong, X Hong, M Gerla - IEEE Military Communications Conference, 2003. ..., 2003

[Cited by 24](#) - [Related articles](#) - [BL Direct](#) - [All 12 versions](#)

Cryptographic solution to a problem of access control in a hierarchy

SG Akl, PD Taylor - ACM Transactions on Computer Systems (..., 1983 - portal.acm.org

... crypton--Data Encryption Standard (DES); **public-key** cryptosystems. ... Furthermore, this protection does not apply only to files that are stored in a central computer memory, but also to messages **broadcast** on a communication network using telephone lines or **radio** waves. ...

[Cited by 308](#) - [Related articles](#) - [All 2 versions](#)

[PDF] Trust management and proof-carrying code in secure **mobile-code** ...

J Feigenbaum, P Lee - ... Workshop on Foundations for Secure **Mobile** ..., 1997 - Citeseer

... A may require metadata signed by C that provides a valid **public key** for B , a ... This would be accomplished by enclosing fragments of **mobile** code into each network packet, to ... networks seem to provide a means for better support multicast and **broadcast** applications, essentially ...

[Cited by 36](#) - [Related articles](#) - [View as HTML](#) - [All 20 versions](#)

An optimized protocol for **mobile** network authentication and security

X Yi, E Okamoto, KY Lam - ... **Mobile** Computing and Communications ..., 1998 - portal.acm.org

... tention as it represents one of the earliest solution employ- ing a combination of both private-key and **public-key** encryp- tion. ... In the same article, Zheng proposed an authentication and key distribution protocol that utilized a **broadcast** channel for a **mobile** user authenticating ...

[Cited by 14](#) - [Related articles](#) - [All 3 versions](#)

[CITATION] MANETconf: Configuration of hosts in a **mobile** ad hoc network

S Nesargi, R Prakash - IEEE INFOCOM 2002. Twenty-First Annual Joint ..., 2002

[Cited by 316](#) - [Related articles](#) - [BL Direct](#) - [All 25 versions](#)

[CITATION] Conference key distribution schemes for secure digital ...

MS Hwang, WP Yang - IEEE Journal on Selected areas in communications, 1995

[Cited by 38](#) - [Related articles](#) - [BL Direct](#) - [All 3 versions](#)

[PDF] ... : A simple, cheat-proof, credit-based system for **mobile** ad-hoc networks

S Zhong, J Chen, YR Yang - IEEE INFOCOM, 2003 - Citeseer

... where PK0 is the **public key** of the sender. ... As route-discovery **broadcast** can be viewed as a special case of multicast, this approach can also be applied to multicast if ... In the evaluations below, our **mobile** node is a Laptop with an Intel **Mobile** Pentium III processor at 866MHz. ...

[Cited by 605](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 36 versions](#)

Key agreement in ad hoc networks* 1

N Asokan, P Ginzboorg - Computer Communications, 2000 - Elsevier

... These **public key** certificates can allow participants to verify the binding between the IP addresses and keys ... The strongest attacker can disrupt any protocol by jamming the **radio** channel or modifying ... The leader will **broadcast** the message in step 1. The rest of the messages will ...

[Cited by 387](#) - [Related articles](#) - [All 10 versions](#)

[CITATION] LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc ...

S Zhu, S Xu, S Setia, S Jajodia - Distributed Computing Systems Workshops, 2003. ..., 2003

[Cited by 59](#) - [Related articles](#) - [All 19 versions](#)

Weak duplicate address detection in **mobile** ad hoc networks

NH Vaidya - ... international symposium on **Mobile** ad hoc networking ..., 2002 - portal.acm.org

... to the Address Resolution Protocol (ARP), such that ARP replies are sent by a **broadcast**, as opposed ... This paper considers the problem of duplicate address de- tection (DAD) in **mobile** ad hoc networks. ... and it may not be possible to embed the key 3 If **public-key** cryptography is ...

[Cited by 230](#) - [Related articles](#) - [All 26 versions](#)

Strategies for enhancing routing security in protocols for **mobile** ad hoc networks* 1

L Venkatraman, DP Agrawal - Journal of Parallel and Distributed ..., 2003 - Elsevier

... Moreover, this authority can be well protected since it is not **mobile** like the other nodes. ... has elapsed, and if the node mobility are relatively high, each node might need to store the **public key** of large ... Denial of service: This can be done by generating false **broadcast** packets like ...

[Cited by 45](#) - [Related articles](#) - [BL Direct](#) - [All 6 versions](#)

Cellular telephony authentication arrangement

JA Reeds III, PA Treventi, IH Yu - US Patent 5,204,902, 1993 - Google Patents

... which rule out the classical approach also rule out the **public key** approach. ... A-key, MINI and MIN2 designations and whal- ers and cellular **radio** providers interconnected ... the registration sequence when the on some preassigned frequency channel (**broadcast mobile** unit goes ...

[Cited by 25](#) - [Related articles](#) - [All 3 versions](#)

[PDF] Security issues in a future vehicular network

M El Zarki, S Mehrotra, G Tsudik, N ... - European Wireless, 2002 - Citeseer

... Also, vehicles communicating in an ad hoc network **broadcast** their data, thus, pair-wise (or group-wise) key distribution is ... issues: a related concern in many **mobile** networks is the low CPU speed of the **mobile** node. ... Certification Infrastructure (PKI): **public key** digital signatures ...

[Cited by 90](#) - [Related articles](#) - [View as HTML](#) - [All 9 versions](#)

[PDF] **Mobile** ad hoc networking: imperatives and challenges

I Chlamtac, M Conti, JJN Liu - Ad Hoc Networks, 2003 - Citeseer

... networking applications can be traced back to the DARPA Packet **Radio** Network (PRNet ... and store- and-forward routing, and its possible application in **mobile** wireless environment. PRNet features a distributed architecture consisting of network of **broadcast** radios with minimal ...

[Cited by 497](#) - [Related articles](#) - [View as HTML](#) - [All 31 versions](#)

A new anonymous conference key distribution system based on the elliptic curve ...

CC Yang, TY Chang, MS Hwang - Computer Standards & Interfaces, 2003 - Elsevier

... An adversary who intends to reveal a secret key x_i from its corresponding **public key** Q_i will ... 3. M.-S. Hwang and WP Yang, Conference key distribution protocols for digital **mobile** communication systems ... 4. T. Hwang and JL Chen, Identity-based conference key **broadcast** system ...

[Cited by 19](#) - [Related articles](#) - [All 6 versions](#)

Secure multicast in wireless networks of **mobile** hosts: protocols and issues

D Bruschi, E Rosti - **Mobile** Networks and Applications, 2002 - Springer

... $M_{si} \subseteq M$ is the set of **mobile** hosts in the cell con- trolled by support station s_i metric key pair associated with entity j in the PKI, where p_j is the **public key** and p^{-1}_j is the private ... or a group of senders/receivers, eg, a subset of S or of M , in case of multicast or **broadcast** messages ...

[Cited by 58](#) - [Related articles](#) - [BL Direct](#) - [All 7 versions](#)

[PDF] Energy-efficient and low-latency key management for sensor networks

DW Carman, BJ Matt, GH Cirincione - ... Security Research Journal, 2003 - isso.sparta.com

... recent investigation in establishing keys to secure link-layer broadcasts for a prototype Army

sensor network **radio** reveals that ... other members Uni-cast to a single member 1 6 5 4 3 2 Group leader **broadcast** its certificate (and its ephemeral **public key**) Group members ...

[Cited by 35](#) - [Related articles](#) - [View as HTML](#) - [All 3 versions](#)

[PDF] Securing **mobile** ad hoc networks

P Papadimitratos, ZJ Haas - Handbook of Ad Hoc Wireless Networks, 2002 - Citeseer

... A second proposal to secure AODV makes use of **public key** cryptography as well and ... The Secure Routing Protocol The Secure Routing Protocol (SRP) [17] for **mobile** ad hoc ... Communication takes place over a **broadcast** medium, and it is assumed that malicious nodes, which ...

[Cited by 35](#) - [Related articles](#) - [View as HTML](#) - [All 9 versions](#)

[PDF] Ubibay: An auction system for **mobile** multihop ad-hoc networks

H Frey, JK Lehnert, P Sturm - Workshop on Ad hoc Communications and ..., 2002 - Citeseer

... It is assumed that a central certification authority (CA) outside of the **mobile** ad-hoc network exists ... verify the authenticity of the **public key** by checking the certificate with the **public key** of the ... Buffer fragments are appended to the **broadcast** message as long as its length is less or ...

[Cited by 15](#) - [Related articles](#) - [View as HTML](#) - [All 18 versions](#)

[PDF] Preventing selfishness in open **mobile** ad hoc networks

H Miranda, L Rodrigues - Proc. Seventh CaberNet Radicals Workshop, 2002 - Citeseer

... However, there is a significant difference between the fixed and the **mobile** environment. ... The modules use a **Public Key** Infrastructure (PKI) to ensure the authentication of the tamper ... by being suspicious on the incoming selfish- ness alerts that other nodes **broadcast** and relying ...

[Cited by 28](#) - [Related articles](#) - [View as HTML](#) - [All 9 versions](#)

[CITATION] ... for distributed and dynamic network managementbased on **mobile** ...

D Gavalas, D Greenwood, M Ghanbari, M O'Mahony - 1999 IEEE International ..., 1999

[Cited by 54](#) - [Related articles](#) - [BL Direct](#) - [All 8 versions](#)

A practical and secure fault-tolerant conference-key agreement protocol

WG Tzeng - Public Key Cryptography, 2000 - Springer

... to establish a com- mon conference key K such that all their communications thereafter are encrypted with the key K. In this paper we propose a practical and prov- ably secure fault-tolerant conference-key agreement protocol under the authenticated **broadcast** channel model. ...

[Cited by 35](#) - [Related articles](#) - [BL Direct](#) - [All 5 versions](#)

[PDF] Analysis of security and privacy in **mobile** IP

A Fasbender, D Kesdogan, O Kubitz - 4th International Conference on ..., 1996 - Citeseer

... Is no expectation of guaranteed privacy in cellular telephone networks, which **broadcast** their signals ... recommends that if absolute protection from traffic analysis is required, the **mobile** node can ... the help of so-called mixes is a technique based on **public key** cryptography mainly ...

[Cited by 47](#) - [Related articles](#) - [View as HTML](#) - [All 7 versions](#)

[CITATION] New multiparty authentication services and key agreement protocols

G Ateniese, M Steiner, G Tsudik - IEEE Journal on Selected Areas in ..., 2000

[Cited by 271](#) - [Related articles](#) - [BL Direct](#) - [All 23 versions](#)

Anonymous channel and authentication in wireless communications

WS Juang, CL Lei, CY Chang - Computer communications, 1999 - Elsevier

... Due to the roaming, dynamic channel assignment and **broadcasting** features of **mobile** communications, if a ... Y. Also, let K_{vh} be the secret key shared by H and V, HID be H's identification number, $\{m\}_e$ denote the ciphertext of m encrypted using Rabin's **public key** e ...

[Cited by 48](#) - [Related articles](#) - [All 9 versions](#)

Public-key support for group collaboration

C Ellison, S Dohrmann - ACM Transactions on Information and ..., 2003 - portal.acm.org
 ... that we address and that we see in our daily lives is on **mobile** machines, often ... whether the member is connected and, if so, its network address and its **public key**) would be ... 802.11 ad hoc mode, in NGC implementations so far), presence information is gathered by **broadcast**. ...
[Cited by 31](#) - [Related articles](#) - [All 2 versions](#)

Method and system for a **public key** cryptosystem having proactive, robust, and ...
 A Herzberg, SM Jarecki, HM Krawczyk, MM ... - US Patent ..., 1997 - Google Patents
 ... "How to Withstand **Mobile** Virus Attacks ... AN UPDATING POLYNOMIAL 512 COMPUTE SHARES FROM POLYNOMIAL 514 / CREATE MESSAGE FROM SHARES 516 PICK PRIVATE KEY 518 COMPUTE CORRESPONDING **PUBLIC KEY** 520 **BROADCAST** MESSAGE PAIR ...
[Cited by 11](#) - [Related articles](#) - [All 3 versions](#)

Secure **mobile** agents on ad hoc wireless networks
 E Sultanik, D Artz, G Anderson, M Kam, W Regli ... - The Fifteenth Innovative ..., 2003 - aaai.org
 ... The security framework uses a combination of symmetric and **public-key** cryptography to support encrypted ... state; make deci- sions about their itineraries (ie, if they are **mobile** agents) based on ... may not mirror the connectivity of the network— hence, a **broadcast** message from ...
[Cited by 30](#) - [Related articles](#) - [All 9 versions](#)

... , wireless coverage and cooperation on data dissemination among **mobile** devices
 M Papadopoul, H Schulzrinne - ... international symposium on **Mobile** ..., 2001 - portal.acm.org
 ... the source and the destina- tion are required to have PGP in order to encrypt (using the **public key**) and then ... with a constant speed uniformly selected from (0 m/s, 1.5 m/s). When a **mobile** host reaches ... The **broadcast** is scheduled at a random time selected from the on interval. ...
[Cited by 214](#) - [Related articles](#) - [All 34 versions](#)

[CITATION] Mobile agent middleware for **mobile** computing
 P Bellavista, A Corradi, C Stefanelli - Computer, 2001
[Cited by 167](#) - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)

[PDF] Security and privacy in **radio**-frequency identification devices
 SA Weis - 2003 - Citeseer
 ... Page 20. Fundamentally, readers are quite simple devices and could be incorporated into **mobile** ... a narrow band of **radio** frequencies specified by regulation agencies such as the Federal ... the collision. The reader will then **broadcast** a bit indicating whether tags who **broadcast** ...
[Cited by 247](#) - [Related articles](#) - [View as HTML](#) - [All 26 versions](#)

Towards flexible credential verification in **mobile** ad-hoc networks
 SL Keoh, E Lupu - ... international workshop on Principles of **mobile** ..., 2002 - portal.acm.org
 ... Note that since all the credentials in a CAS may be confirmed by assertions from the same source and since the recipient has the **public key** of the ... In order to enhance the revocation capabilities in **mobile** ad-hoc network, issuers of ASSs may choose to **broadcast** to peers ...
[Cited by 20](#) - [Related articles](#) - [All 11 versions](#)

[PDF] A secure routing protocol for ad hoc networks
 B Dahill, BN Levine, E Royer, C Shields - ... , Tech. Rep. UM-CS-2001-037, 2001 - scss.tcd.ie
 ... Additionally, **mobile** nodes in the managed-open environment reside within some com- mon context or geographic proximity ... signed by T . All nodes must maintain fresh certificates with the trusted server and must know T 's **public key**. ... A → **broadcast** : [RDp, lpK, certa, Na, t]Ka- (2 ...
[Cited by 238](#) - [Related articles](#) - [View as HTML](#) - [All 10 versions](#)

[PDF] Cooperative routing in **mobile** ad-hoc networks: Current efforts against ...
 S Buchegger, JY Le Boudec - Lecture Notes on Informatics, **Mobile** ..., 2002 - Citeseer
 ... wireless links are vulnerable to jamming and by their inherent **broadcast** nature facilitate ... refreshing

for distributed certification authorities for key management in **mobile** ad-hoc ... Localized certification based on the **public key** infrastructure (PKI) with certification- authority and ...

[Cited by 33](#) - [Related articles](#) - [View as HTML](#) - [All 18 versions](#)

[CITATION] Achieving user privacy in **mobile** networks

B Askwith, M Merabti, Q Shi, K Whiteley - Computer Security Applications ..., 1997

[Cited by 25](#) - [Related articles](#) - [All 7 versions](#)

[PDF] **Mobile** agents and security

MS Greenberg, JC Byington, DG Harper - IEEE Communications Magazine, 1998 - ic.uiff.br

... The recipients of this **broadcast** include the auto-configuration server on β and the two malicious **mobile** ... Authenticating Credentials — A **mobile** agent is digitally signed by one or more parties using one of a number of algorithms, such as a **public key** signature algorithm ...

[Cited by 170](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 4 versions](#)

[CITATION] Key establishment in large dynamic groups using one-way function ...

AT Sherman, DA McGrew - IEEE transactions on Software Engineering, 2003

[Cited by 173](#) - [Related articles](#) - [BL Direct](#) - [All 10 versions](#)

[CITATION] Security requirements and protocols for a **broadcast** scenario

S Kent - Communications, IEEE Transactions on [legacy, pre- ..., 1981

[Cited by 20](#) - [Related articles](#)

The design and implementation of a private message service for **mobile** computers

DA Cooper, KP Birman - Wireless Networks, 1995 - Springer

... As with most **public key** encryption schemes, RSA can also be used to sign messages. ... Since messages are **broadcast** to every computer, recipient anonymity is also guaranteed. ... This technique is also not well suited for **mobile** computers which may frequently disconnect from the ...

[Cited by 17](#) - [Related articles](#) - [All 9 versions](#)

[CITATION] ... and foes: Preventing selfishness in open **mobile** ad hoc networks

H Miranda, L Rodrigues - ..., 2003. Proceedings. 23rd International Conference on, 2003

[Cited by 26](#) - [Related articles](#) - [All 8 versions](#)

[CITATION] New directions in cryptography

W Diffie, M Hellman - IEEE Transactions on information Theory, 1976

[Cited by 7514](#) - [Related articles](#) - [All 151 versions](#)

[CITATION] Direct **broadcast** satellite communications: an MPEG enabled service

DC Mead - 2000 - Addison-Wesley

[Cited by 8](#) - [Related articles](#)

[CITATION] Secure aggregation for wireless networks

L Hu, D Evans - Applications and the Internet Workshops, 2003. ..., 2003

[Cited by 212](#) - [Related articles](#) - [All 21 versions](#)

An authentication framework for hierarchical ad hoc sensor networks

M Bohge, W Trappe - Proceedings of the 2nd ACM workshop on ..., 2003 - portal.acm.org

... nodes that relay information from sensor nodes to access points, and (D) low-powered **mobile** sensor nodes ... system for low-powered devices, we need a certificate structure that does not employ **public key** cryptography. TESLA [12] is a **broadcast** authentication technique that ...

[Cited by 89](#) - [Related articles](#) - [All 20 versions](#)

Chinese lotto as an exhaustive code-breaking machine

JJ Quisquater, YG Desmedt - COMPUTER., 1991 - computer.org

... In **public-key** cryptosystems, where $K \neq K'$, we call K the **public key** and K' the secret decryption key; publishing K does not endanger the security of the cryptosystem. ... A plaintext-ciphertext pair is **broadcast** regularly by all **radio** and television stations. ...

[Cited by 20](#) - [Related articles](#) - [All 5 versions](#)

The need for decentralization and privacy in **mobile** communications networks

F Stoll - Computers & Security, 1995 - Elsevier

... Security, Vol. 74, No. 6 that is specified in the location information. This element then ciphers the call request with the **public key** of the **mobile** station and initiates a **broadcast** of the call request in its area. Only the ...

[Cited by 10](#) - [Related articles](#) - [All 9 versions](#)

Stop-and-go-MIXes providing probabilistic anonymity in an open system

D Kesdogan, J Egner, R Büschkes - Information Hiding, 1998 - Springer

... Our answer to this question follows a probabilistic model. We define this model in section 3 analogous to the one used for **public key** cryptosystems. ... non-ambiguous E E Fig. 1. Recipient anonymity by **broadcast** and addressing attributes ...

[Cited by 168](#) - [Related articles](#) - [All 13 versions](#)

[CITATION] Satellites, packets, and distributed telecommunications: a compendium ...

RD Rosner - 1984 - Lifetime Learning Pub

[Cited by 7](#) - [Related articles](#) - [Library Search](#)

A wireless public access infrastructure for supporting **mobile** context-aware IPv6 ...

A Friday, M Wu, S Schmid, J Finney, K ... - ... on Wireless **mobile** ..., 2001 - portal.acm.org

... The **broadcast** protocol is one of the key mechanisms for promoting the scalability of GUIDE ... In **Mobile** IPv6 this limitation implies that a potential attacker must remain co-located with ... impersonation of the authentication server, the payload is encrypted using the **public key** of the ...

[Cited by 8](#) - [Related articles](#) - [All 10 versions](#)

Google

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

"public key" broadcast (mobile OR radio)

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

Web Images Videos Maps News Shopping Gmail more ▾

Sign in

Google scholar

"public key" broadcast (mobile OR radio) decrypt

Search

[Advanced Scholar Search](#)
[Scholar Preferences](#)

- ☒ Search only in Engineering, Computer Science, and Mathematics.
☐ Search in all subject areas.

Scholar

Articles and patents

- 2003

include citations

Results 1 - 100 of abc

... anonymous on demand routing with untraceable routes for **mobile** ad-hoc networks

J Kong, X Hong - ... of the 4th ACM international symposium on **Mobile** ..., 2003 - portal.acm.org

... The first one is a naive porting of MIX-Net to **mobile** ad hoc networks. ... Compared to ANODR-PO, ANODR-BO ensures that no **public key** operation is executed during RREQ ... 3 shows the case where anonymous route discovery depends completely on local **broadcast** with trap ...

[Cited by 291](#) - [Related articles](#) - [All 27 versions](#)

[PDF] Secure routing for **mobile** ad hoc networks

P Papadimitratos, ZJ Haas - SCS Communication Networks and ..., 2002 - Citeseer

... Abstract The emergence of the **Mobile** Ad Hoc Networking (MANET) technology advocates self-organized ... could be instantiated, for example, by the knowledge of the **public key** of the ... Finally, the **broadcast** nature of the **radio** channel mandates that each transmission is received ...

[Cited by 957](#) - [Related articles](#) - [View as HTML](#) - [All 51 versions](#)

Digital rights management for **content** distribution

Q Liu, R Safavi-Naini, NP Sheppard - Proceedings of the ..., 2003 - portal.acm.org

... though a client/server system, super-distribution 2, digital audio/video **broadcasting**, or CDs ... corresponding **public key** is used as the player's identifier when requesting a license and the ... digital data processing devices such as PCs, portable music players, **mobile** phones, digital ...

[Cited by 177](#) - [Related articles](#) - [All 22 versions](#)

[CITATION] Preserving privacy in a network of **mobile** computers

DA Cooper, KP Birman - 1995 IEEE Symposium on Security and Privacy, 1995. ..., 1995

[Cited by 88](#) - [Related articles](#) - [BL Direct](#) - [All 23 versions](#)

Digital signets: Self-enforcing protection of digital information (preliminary version)

C Dwork, J Lotspiech, M Naor - ... of the twenty-eighth annual ACM ..., 1996 - portal.acm.org

... pair, or indeed to generate any short string from which, with the aid of the extrication function and other public data, the **content** can be **decrypted**, without revealing information pri- vate to the adversary. We will discuss this connection - and ...

[Cited by 93](#) - [Related articles](#) - [BL Direct](#) - [All 8 versions](#)

Networks without user observability—design options

A Pfitzmann, M Waldner - Advances in Cryptology—EUROCRYPT'85, 1985 - Springer

... for the classical **broadcast** services TV and **radio**, great parts of the life of any user ... Conversely, if you have any invisible addressing scheme, you can do **public key** distribution: If you ... based on superposing sending, channels can then be switched as in normal **broadcast** networks ...

[Cited by 220](#) - [Related articles](#) - [All 8 versions](#)

Multicast security and its extension to a **mobile** environment

L Gong, N Shacham - Wireless Networks, 1995 - Springer

... We also describe an initial architectural design for secure multicast in a **mobile** environment.

We conclude 9 JC Baltzer AG, Science Publishers ... the order of $O(2n)$. The problem we examine here is how to securely **broadcast** a message when **public-key** sys- tems are ...

[Cited by 53](#) - [Related articles](#) - [All 8 versions](#)

[PDF] Security in public **mobile** communication networks

H Federrath, A Jerichow, D Kesdogan, A ... - WISSENSCHAFTLICHE ..., 1995 - Citeseer
... completely anonymous to the network by delivering the message (possibly end-to-end-encrypted) to all stations (**broadcast**). ... Change of encoding of a message can be implemented using a **public-key** cryptosystem. ... 2.2.1 **Mobile Radio** Systems with Reduced Locating-Ability ...

[Cited by 30](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 17 versions](#)

[CITATION] A new set of passive routing attacks in **mobile** ad hoc networks

J Kong, X Hong, M Gerla - IEEE Military Communications Conference, 2003. ..., 2003

[Cited by 24](#) - [Related articles](#) - [BL Direct](#) - [All 12 versions](#)

Cellular telephony authentication arrangement

JA Reeds III, PA Treventi, IH Yu - US Patent 5,204,902, 1993 - Google Patents

... is in the classical approach, the same time constraints which rule out the classical approach also rule out the **public key** approach ... that the **mobile** unit created and transmitted, and the RAND sequence that the serving base station **broadcast** (and which the **mobile** unit incor ...

[Cited by 25](#) - [Related articles](#) - [All 3 versions](#)

[CITATION] ... on "Dynamic participation in a secure conferencescheme for **mobile** ...

SL Ng - IEEE Transactions on Vehicular Technology, 2001

[Cited by 16](#) - [Related articles](#) - [BL Direct](#) - [All 3 versions](#)

[CITATION] A Review of of Watermarking Principles and Practices

IJ Cox, ML Miller, JMG Linnartz, T Kalker - 1999 - IEEE

[Cited by 23](#) - [Related articles](#)

Multimedia player for an electronic **content** delivery system

MM Hurtado, GG Gruse, E Downs, KL ... - US Patent 6,418,421, 2002 - Google Patents

... 9,2002 (54) MULTIMEDIA PLAYER FOR AN ELECTRONIC **CONTENT** DELIVERY SYSTEM (75) Inventors: Marco M. Hurtado, Boca Raton; George Gregory Gruse, Lighthouse Point; Edgar Downs, Fort Lauderdale; Kenneth Louis Milsted, Boynton Beach, all of FL (US) (73 ...

[Cited by 12](#) - [Related articles](#) - [All 2 versions](#)

System for tracking end-user electronic **content** usage

GG Gruse, JJ Dorak Jr, KL Milsted - US Patent 6,389,538, 2002 - Google Patents

... 11/1997 4/1998 G06F/17/60 G06F/11/30 G06F/12/14 G06F/11/30 OTHER PUBLICATIONS Micali, Silvio, "Fair **Public-Key** Cryptosystems", Labora ... M. Shofi; Fleit, Kain, Gibbons, Gutman & Bongini PL (57) ABSTRACT 705/56 A system for tracking usage of digital **content** on user ...

[Cited by 14](#) - [Related articles](#) - [All 2 versions](#)

[CITATION] On the limits of steganography

RJ Anderson, FAP Petitcolas - IEEE Journal on selected areas in communications, 1998

[Cited by 546](#) - [Related articles](#) - [BL Direct](#) - [All 58 versions](#)

Key management system for digital **content** player

GG Gruse, MM Hurtado, KL Milsted, JB ... - US Patent ..., 2002 - Google Patents

... A digital **content** player for use on a computer system is also provided. The **content** player includes a decrypter that **decrypts** digital **content** data, which was encrypted with a first encrypting key, using a first **decrypting** key so as to produce the **content** data. ...

[Cited by 6](#) - [Related articles](#) - [All 2 versions](#)

Speech and control message encryption in cellular **radio**

JA Reeds III, PA Treventi - US Patent 5,172,414, 1992 - Google Patents

... information to all units within its cell on some preassigned frequency channel (**broadcast** band). ... One approach may be, for example, for the **mobile** unit to scan all channels and ... MIN2 and MINI designations (either in plaintext form or enciphered with a **public key**), permitting the ...

Cited by 11 - Related articles - All 2 versions

[CITATION] Conference key distribution schemes for secure digital ...

MS Hwang, WP Yang - IEEE Journal on Selected areas in communications, 1995

Cited by 38 - Related articles - BL Direct - All 3 versions

Method and apparatus to create encoded digital content

KL Milsted, KD Nguyen, Q Gong - US Patent 6,263,313, 2001 - Google Patents

... 17, 2001 Sheet 1 of 21 **CONTENT** ten V C\J 10 J T-. SECURE CONTAINER PACKER TOOL J V \ CO <M T— x ^C ^f Q \ V CD ^ -J ... 17, 2001 Sheet 4 of 21 i DC CD o H- PLAYER O 1 — O ATERMARKIN **DECRYPTION** CD YLIST GREAT CD RECORDING o 5 o o O 1 DL D. 1 or LU ...

Cited by 9 - Related articles - All 2 versions

... digital **content** for electronic distribution using the identity of the source **content**

KL Milsted, C Kindell, Q Gong - US Patent 6,345,256, 2002 - Google Patents

... 5,2002 (54) AUTOMATED METHOD AND APPARATUS TO PACKAGE DIGITAL **CONTENT** FOR ELECTRONIC DISTRIBUTION USING THE IDENTITY OF THE SOURCE **CONTENT** (75) Inventors: Kenneth Louis Milsted, Boynton Beach; Craig Kindell, Defray Beach; Qing Gong ...

Cited by 10 - Related articles - All 2 versions

[CITATION] Mobile peer membership management to support multimedia ...

SS Kang, MW Mutka - ... , 2003. Proceedings. 23rd International Conference on, 2003

Cited by 6 - Related articles - All 14 versions

Method for delivering electronic content from an online store

R Spagna, KL Milsted, DP Lybrand, E ... - US Patent 6,587,837, 2003 - Google Patents

... Metadata is acquired which has been previously associated with **content**. ... 1,2003 Sheet 4 of 21 01 o _i f Q O cr o PLAYER APPLICATION PY/PLAY CONT A/ATERMARKIN **DECRYPTION** DECODING AYLIST GREAT CD RECORDING o: cr o 1 CO 1 o A ^ i O) LI o LU Q cc LU W ...

Cited by 9 - Related articles - All 2 versions

Satellite based high bandwidth data broadcast

DM Yee, RH Bickley, PJ Zucarelli, TW Keller, ... - US Patent ... , 2000 - Google Patents

... data communications sys- tem in accordance with claim 3, wherein: said **mobile** subscriber unit ... with a unique **decryption** key via said message link by a **public key** encryption system ... 5. A satellite based **broadcast** data communications sys- tem in accordance with claim 1, wherein ...

Cited by 6 - Related articles - All 2 versions

[PDF] Selective encryption of multimedia **content** in distribution networks: ...

X Liu, AM Eskicioglu - ... , Internet & Information Technology (CIIT), USA, 2003 - Citeseer

... Unicasting involves point-to-point communication between a server and a client device, **broadcasting** requires transmitting the same data to the entire client population, and ... A common tool of achieving the protection of the **decryption** key is **public-key** cryptography. ...

Cited by 57 - Related articles - View as HTML - All 7 versions

[CITATION] Multimedia rights management for the multiple devices of end-user

KA Chang, BR Lee - ... , 2003. Proceedings. 23rd International Conference on, 2003

Cited by 4 - Related articles - All 5 versions

The design and implementation of a private message service for mobile computers

DA Cooper, KP Birman - Wireless Networks, 1995 - Springer

... As with most **public key** encryption schemes, RSA can also be used to sign messages. ... Since messages are **broadcast** to every computer, recipient anonymity is also guaran- ... This techni- que is also not well suited for **mobile** computers which may frequently disconnect from the ...

[Cited by 17](#) - [Related articles](#) - [All 9 versions](#)

[CITATION] Achieving user privacy in mobile networks

B Askwith, M Merabti, Q Shi, K Whiteley - Computer Security Applications ..., 1997

[Cited by 25](#) - [Related articles](#) - [All 7 versions](#)

[CITATION] ... management and watermarking of multimedia content for m-commerce ...

F Hartung, F Rammé - IEEE Communications Magazine, 2000

[Cited by 145](#) - [Related articles](#) - [BL Direct](#) - [All 5 versions](#)

Key management system for DVD copyright management

DW Aucsmith - US Patent 5,915,018, 1999 - Google Patents

... MPEG-1 is optimized for CD-ROM, MPEG-2 for **broadcast** quality video, and MPEG-4 for ... communication including but not limited to, a single wire, a multi-wire path, a **radio** frequency or ... This encryption is done with 55 the **public key** of video controller 210 which was received by ...

[Cited by 12](#) - [Related articles](#) - [All 2 versions](#)

Method and system for a public key cryptosystem having proactive, robust, and ...

A Herzberg, SM Jarecki, HM Krawczyk, MM ... - US Patent ..., 1997 - Google Patents

... How to Withstand **Mobile** Virus Attacks ... 6A 626 COMPUTE SUBSHARES 628 **BROADCAST** ENCRYPTED SUBSHARES 630 COMBINE AND VERIFY SUBSHARES ALL SHARES VERIFIED SHARE ... D from E; and 3. E cannot be broken by attacking P. Thus, the **public key** can be ...

[Cited by 11](#) - [Related articles](#) - [All 3 versions](#)

Conditional access and content security method

RR Sullivan, JM Acken, DW Aucsmith - US Patent 6,069,647, 2000 - Google Patents

... through established or later developed techniques such as infrared (IR) and **radio** frequency (RF ... an orbiting satellite, a cable company, a network, a television **broadcast** company and ... either a symmetric key cryp- tographic function, or perhaps, a **public-key** cryptographic function ...

[Cited by 6](#) - [Related articles](#) - [All 2 versions](#)

Method and apparatus for preventing piracy of digital content

PC Kocher, JM Jaffe, BC Jun - US Patent 6,289,455, 2001 - Google Patents

... and CDK generator to Crypto Firewall 520 Verify that address is valid 530 Retrieve value from protected memory Transform with F, 550 560 Return F, result to ICP 570 Final processing of F3 result to produce CDK 580 Return CDK to playback device 590 **Decrypt content** End) ...

[Cited by 6](#) - [Related articles](#) - [All 4 versions](#)

... of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key ...

CF Grecas, SI Maniatis, IS Venieris - **Mobile** Networks and Applications, 2003 - Springer

... data, using the VLR's **public key**, see figure 3, possibly emitted on the **Broadcast** Channel (BCH ... [5] C. Adams and S. Lloyd, Understanding **Public-Key** Infrastructure (New ... His research interests are directed to the fields of the 2nd, 2.5/3rd generation **mobile** networks, especially on ...

[Cited by 26](#) - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)

Digital content protection method and apparatus

PC Kocher, JM Jaffe, BC Jun - US Patent App. 09/948,473, 2001 - Google Patents

... and CDK generator to CryptoFirewall 520 Verify that address is valid 530 Retrieve value from protected memory 550 Transform with F 560 Return F 3 result to ICP 570 Final processing of F3 result to produce CDK 580 Return CDK to playback device 590 **Decrypt content** Page 7. ...

[Cited by 3](#) - [Related articles](#) - [All 4 versions](#)

[PDF] Copy protection for DVD video

JA Bloom, IJ Cox, T Kalker, JPMG Linnartz, ML ... - Proceedings of the ..., 1999 - Citeseer
 ... is included to support such uses as time shift- ing, where a copy of **broadcast** media is ... so they can send encrypted data to one another that no other devices can **decrypt**. ... Signatures and Diffie-Hellman Key Exchange using a 160-bit elliptic curve **public key** cryptosystem compat ...
[Cited by 178](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 35 versions](#)

SPINS: Security protocols for sensor networks

A Perrig, R Szewczyk, JD Tygar, V Wen, DE Culler - Wireless networks, 2002 - Springer
 ... **Keywords:** secure communication protocols, sensor networks, **mobile** ad hoc networks, MANET, authentication of wireless ... instruction flash 512 bytes RAM 512 bytes EEPROM Communication 916 MHz **radio** Bandwidth 10 ... μ TESLA provides authentication for data **broadcast**. ...
[Cited by 2052](#) - [Related articles](#) - [BL Direct](#) - [All 163 versions](#)

[CITATION] Preserving Privacy in a Network of **Mobile** Computers

DACKP Birman - ... on Security and Privacy: May 8-10 ..., 1995 - IEEE Computer Society Press
[Cited by 2](#) - [Related articles](#) - [All 2 versions](#)

[CITATION] A secure flash card solution for remote access for **mobile** workforce

T Kato, T Tsunehiro, M Tsunoda, J Miyake - IEEE Transactions on Consumer ..., 2003
[Cited by 2](#) - [Related articles](#) - [BL Direct](#)

eXtensible **content** protection

F Pestoni, C Drews - Proceedings of the eleventh ACM international ..., 2003 - portal.acm.org
 ... which is orders of magnitude more efficient than techniques based on **public key** cryptography [1 ... 4. HOME NETWORKS IBM Research, a leader in **broadcast** encryption, has developed a ... a main residence and a summer home, download/playback on **mobile** devices including ...
[Cited by 1](#) - [Related articles](#) - [All 2 versions](#)

[PDF] Analysis of security and privacy in **mobile** IP

A Fasbender, D Kesdogan, O Kubitz - 4th International Conference on ..., 1996 - Citeseer
 ... that there is no expectation of guaranteed privacy in cellular telephone networks, which **broadcast** their signals ... the possibility of guessing $X = M$ by checking $K(X) = K(M)$ using the **public key** K . However ... agents before it is delivered to the FA and then forwarded to the **mobile** node ...
[Cited by 47](#) - [Related articles](#) - [View as HTML](#) - [All 7 versions](#)

[PDF] A multi-level, multicast web caching system for interconnected lmds ...

H Linder, HD Clausen, W Stering - IST **Mobile** and Wireless ..., 2002 - Citeseer
 ... Node B **decrypts** the hash with node A's **public key** and compares the **decrypted** hash with the signature contained in the packet. ... Internet over Direct **Broadcast** Satellites. ... Route Diversity in an Interconnected LMDS Network, IST **Mobile** Summit 2001, Sitges, Spain, 2001. ...
[Cited by 1](#) - [Related articles](#) - [View as HTML](#) - [All 5 versions](#)

Method for coordinating the operation of **mobile** equipment

NJ King, PJ Kozdon - US Patent 6,275,697, 2001 - Google Patents
 ... The method depends upon the **mobile** lower priority system listening to ... beacon broadcasts an encrypted signature that inhibits persons wishing to **broadcast** a fraudulent ... this approach, any reasonable encrypting system may be used including "**public key**" encryption systems. ...
[Cited by 1](#) - [Related articles](#) - [All 5 versions](#)

[BOOK] Secure **broadcast** communication in wired and wireless networks

A Perrig, JD Tygar - 2003 - books.google.com
 ... 70 4.4.3 Example: Real-time stock quotes 70 4.4.4 Efficient **Public-Key** Distribution 73 ... We present some **broadcast** applications here, and we discuss them in greater detail later in this ... Digital TV and digital **radio** dis- tributed over the Internet are becoming increasingly popular. ...

[Cited by 107](#) - [Related articles](#) - [Library Search](#) - [All 2 versions](#)

Service provision authentication protocol

JA Reeds III, PA Treventi - US Patent 5,153,919, 1992 - Google Patents

... with the base station by concatenating a secret pass- word and the most recently **broadcast** random number ... 50 rule out the **public key** approach. ... DETAILED DESCRIPTION In a **mobile** cellular telephone arrangement there are many **mobile** telephones, a much smaller number of ...

[Cited by 28](#) - [Related articles](#) - [All 3 versions](#)

Anonymous channel and authentication in wireless communications

WS Juang, CL Lei, CY Chang - Computer communications, 1999 - Elsevier

... Due to the roaming, dynamic channel assignment and **broadcasting** features of **mobile** communications, if a subscriber broadcasts ... i ,f(Key i),e r ,n h ,e h ,h()) in his handset (**mobile** unit ... All messages, except HID and N 1 , will be encrypted by the H's Rabin's **public key** for privacy ...

[Cited by 48](#) - [Related articles](#) - [All 9 versions](#)

[CITATION] Dynamic participation in a secure conference scheme for ...

MS Hwang - IEEE transactions on vehicular technology, 1999

[Cited by 46](#) - [Related articles](#) - [BL Direct](#) - [All 5 versions](#)

[CITATION] Anonymous communication in practice

C Boesgaard - Department of Computer Science, University of ..., 2003

[Cited by 3](#) - [Related articles](#)

WAR: Wireless anonymous routing

M Blaze, J Ioannidis, AD Keromytis, T Malkin, A ... - Security Protocols, 2003 - Springer

... To avoid **public key** oper- ations on a per-packet basis, onion routers use per-connection symmetric ... well as a suite of protocols that provides basic anonymity functions in local **broadcast** networks. ... 24 (1981) 84–88 2. Ostrovsky, R., Yung, M.: How to withstand **mobile** virus attacks ...

[Cited by 4](#) - [Related articles](#) - [BL Direct](#) - [All 5 versions](#)

System and method for using DRM to control conditional access to DVB content

J Alve, A Ikonen, M Kangas, T ... - US Patent App. 10/705,449, 2003 - Google Patents

... or know how to encrypt **content** so that the UK can **decrypt** it, ie **public key** cryptography. ... sending a request for **content** rights usage from a **mobile** terminal over a **mobile** network. ... A system for protecting digital video **broadcast** con- tent comprising: a **mobile** network; a computer ...

[All 3 versions](#)

Method and system for purchasing broadcast content

B Huddelston, DC Loose, MP Nuttal - US Patent App. 10/192,436, 2002 - Google Patents

... 1 illustrates the front portion 10 of an auto- **mobile** with its dashboard 20 including a ... type of protection that suits his design and may use either **public key** encryption, private ... but this method of identifying **content** becomes somewhat confusing when a **radio broadcast** may include ...

[All 4 versions](#)

Access to encrypted broadcast content

D Husemann, M Nidd - US Patent App. 10/497,816, 2002 - Google Patents

... US 2005/0100161 A1 May 12, 2005 over the **broadcast** channel. ... embodiment, the recently introduced smart card solution is broadened to other **mobile** units, such as ... an exchangeable storage medium, this storage medium can store the receiver subsystem's **public key** and a ...

[All 6 versions](#)

Secure registration for a multicast-broadcast-multimedia system (MBMS)

F Grilli, L Casaccia, J Semple, PA ... - US Patent App. 10/ ..., 2003 - Google Patents

... 10. The method of claim 1, wherein the PK is provisioned by using a **public key**. 11. The method

of claim 1, wherein the BAK is provided by using a **public key**. 12. A method of obtaining secure registration by a **mobile** station in a multicast-**broadcast**-multimedia system ...

[All 3 versions](#)

[CITATION] ... Project Report Addressing Mobile IP Security Issues with a Public Key ...
IP Addressing **Mobile** - 2000

[Related articles](#)

[PDF] System LSIs with Cryptographic Functions and Their Applications

K Takaragi, K Nakada, T Yamada, T Arai, H Hara - Hitachi Review, 1999 - hitachi.com

... The CPU processes at high speed both secret-key cryptography, such as Hitachi's MULTI2 and the US standard DES, and **public-key** cryptography, such as RSA and ... LSIS FOR DIGITAL **BROADCAST** SYSTEMS †3 Digital **Broadcast** and Cryptography **Radio** and television ...

[View as HTML](#) - [All 2 versions](#)

New channels, old concerns: scalable and reliable data dissemination

C Allison, D McPherson, D Husemann - Proceedings of the 9th ..., 2000 - portal.acm.org

... In contrast to the **public key** style of cryptography, a symmetrical Remote Key algorithm, BEAST RK [19], is used. ... 2000, 16. Eureka_147_Partners, **Radio Broadcasting** Systems: Digital Audio **Broadcast** to **Mobile**, Portable and Fixed Receivers, 1997, European ...

[Related articles](#) - [All 13 versions](#)

Method and apparatus for distributing keys for **decrypting** and re-encrypting ...

GL Graunke - US Patent App. 09/896,613, 2001 - Google Patents

... **content**. It uses a **public key** encryption scheme. ... direct Page 7. US 2003/0005285
Al Jan. 2, 2003 **broadcast** satellite system, a **radio** digital television system or it can be through a wide area network including the Internet. **Content** ...

[All 3 versions](#)

Method for securely distributing & updating digital **content**

TN Giaccherini, MA Sturza, JR Stuart - US Patent App. 09/948,021, 2001 - Google Patents

... Selected least significant bits of data, controlled by customer **public key**, are altered ... relay packets of digitized data from ground stations to customers using fixed, **mobile** or handheld ... VHP and UHF tele- vision **broadcast**, AM **broadcast** and FM **broadcast** stations are usable for ...

Systems and methods for providing local **broadcast** of an event to event attendees

TJ Parry, R Seseek - US Patent App. 10/264,607, 2002 - Google Patents

... 110 comprise portable viewing devices such as personal digital assistants (PDAs), **mobile** telephones, and ... the attendee transmits the attendee's **public key** to the local **broadcast** control program ... The attendee's **public key** is then used to encrypt the **content** (data packets) such ...

Method for verifying validity of domestic digital network key

C Le Buan, R Ksontini - US Patent App. 10/521,451, 2003 - Google Patents

... [0004] The original contents arrive in house by different sources: it can be transmitted by **radio** channel, by ... all cryptograms: [0054] 1).—The terminal module (CT) of the first device transmits its **public key** (PK) to ... [0055] 2).—The converter module (CC) (or the **broadcast**- ing device ...

[All 5 versions](#)

System and method for secure distribution of digital **content** via a network

SP Morgan - US Patent App. 10/136,828, 2002 - Google Patents

... 194 (57) ABSTRACT The invention defines a system and method for **broadcasting** high quality ... broad- cast in support of services such as digital **radio** or television ... THE ENCRYPTED CONTROL INFORMATION ^-1410 USE PRIVATE KEY TO **DECRYPT** CONTROL INFORMATION ...

[All 2 versions](#)

Mobile device and method for providing certificate based cryptography

GA Bellipady, DT Michau - US Patent App. 10/741,510, 2003 - Google Patents

... CERTIFICATE REVOCATION NOTIFICATION TO A PLURALITY OF **MOBILE** DEVICES USING A **BROADCAST** CHANNEL 256 ... updating a certificate revocation status of a certificate in a **mobile** device ... The **public key**, known to everyone, allows anyone to encrypt a message for a ...

[All 5 versions](#)

Secure satellite communications system

PF Alexander - US Patent 6,487,294, 2002 - Google Patents

... communications system according to claim 1, wherein the stations are fixed, portable, or **mobile**. ... other system status and operational information on a common signaling **broadcast** channel. ... to claim 1, wherein the encryption/**decryption** technique is a **public key** encryption/private ...

[All 4 versions](#)

Rental system for a playback device

M Ohmori, Y Futa, M Tatebayashi - 2002 - freepatentsonline.com

... 90 receives the billing device **public key** (step S552), and stores the received **public key** (step S553). ... player 40 may be connected to time source device 50 via a **mobile** phone network ... Alternatively, time source device 50 may **broadcast** current time via a digital **broadcast** network ...

Portable content by way of a set-top device/home-gateway

R Safadi - US Patent App. 09/827,166, 2001 - Google Patents

... The receiver/playback device includes a stationary device, a **mobile** device, a portable ... Furthermore, the audiovisual programming, analog programming, digital **broadcast** or on-demand MPEG-2 ... When a **Public-Key** Encryption for- mat is used for encryption and **decryption**, the ...

... of return link for hand-off between coverage areas being traversed by a mobile ...

DS Parkman, GV Stephenson, RA ... - US Patent App. 09/ ..., 2001 - Google Patents

... Telecommunica- tions Union (ITU) for fixed satellite services (FSS) or **Broadcast** Satellite Services ... by reference into the present application), wrapped in the asymmetric **public key** of the ... A method for coordinating a hand-off of communica- tion from a **mobile radio** frequency (RF ...

[All 6 versions](#)

Digital content rendering device and method

DH Vogler, EA Chemaity, EA Dabbish, TS ... - US Patent App. 10/ ..., 2003 - Google Patents

... In some cases the **content** rendering device 100 is **mobile** and its location can vary ... For example, the second level of rendering could be one for which the television **broadcast** is shown ... the set of specified locations, and wherein the **content** key is encrypted with a **public key** of the ...

[All 2 versions](#)

... for enabling connected devices to access encrypted audio and visual content

PC Kocher, JM Jaffe, BC Jun - US Patent App. 10/695,256, 2003 - Google Patents

... **public key** and/or symmetric cryptography to re-en- crypt the derived key data for another device, and provides the re-encrypted key data to the decoding device. The decoding device then uses cryptographic values derived from the re-encrypted key data to **decrypt** the **content**. ...

[Related articles](#) - [All 3 versions](#)

Method and system for content distribution

J Alve - US Patent App. 10/691,621, 2003 - Google Patents

... Upon a determination that any conditions for approving such a request are satisfied, the authorized agent **decrypts** a super- distribution key with its private key, and encrypts the resultant **content** key with the **public key** of the second device. ...

[All 5 versions](#)

Automatic commercial skipping service

RB Sagar - US Patent App. 09/927,305, 2001 - Google Patents

... [0007] International application WO 99/37045 proposes a digital **radio broadcast** system providing ...
The provider 102 encrypts the timestamps 316 using this **public key**. ... a second field 312 and a third field 314 indicating respective beginning and end of **broadcast of content** 123. ...

[All 5 versions](#)

Distributing digital content

GD Sasaki, MC Hans - US Patent App. 09/741,725, 2000 - Google Patents

... 5A **Content** Purchased? Yes Encrypt **Content** Package with **Content** Key Encrypt Transfer File with User's **Public Key** ,164 Transmit Transfer File to Recipient User ,166 **Decrypt Content** Package and Embed User ID X 162 FIG. 5B Page 6. Patent Application Publication Jun. ...

[All 2 versions](#)

System and method of distributing and controlling rights of digital content

Y Tsukamura - US Patent App. 10/447,404, 2003 - Google Patents

... [0023] Transmission between components 110-150 may be via wireless communication such as, for example, **mobile** telecommunications link ... [0056] A **public key** of licensee ... or on storage media, such as CD-ROM, through the mail or from Internet sites or other **broadcast** centers ...

System and method for satellite broadcasting and receiving encrypted television ...

DC Cromer, JJ Jankowsky, HJ Locker, AL ... - US Patent App. 10/ ..., 2003 - Google Patents

... IN DATABASE 112 PROGRAM PROVIDER ENCRYPTS SECRET KEY WITH RECEIVER **PUBLIC KEY** PROGRAM PROVIDER ... 1 is a block diagram of a Direct **Broadcast** Satellite System (DBS), in ... These analog signals are provided as inputs to a **radio** frequency (RF) modulator ...

[All 2 versions](#)

... for wireless delivery, storage, and playback of multimedia content on mobile ...

S Cohn, MB Ross - US Patent App. 10/040,617, 2001 - Google Patents

... Several companies currently utilize this model to deliver services such as Internet **radio** or TV to ... for a generic player application to play high quality media **content** on a **mobile** device: ... The **public key** is encoded into the media file from the **content** provider and **decrypted** at the ...

[All 2 versions](#)

Secure electronic content distribution on CDS and DVDs

MM Hurtado, KL Milsted, GG Gruse, E ... - US Patent App. 09/ ..., 1999 - Google Patents

... A user selects from the metadata associated **content** to **decrypt** and the end user system establishes a secure connection with an authentication authority for **decrypting** the **content**. The end user system receives a secure container ...

[Cited by 4](#) - [Related articles](#) - [All 4 versions](#)

Prospects of Secure Real-Time Video Transmission over CDPD Networks

FG Farid Hatefi, G Seckin - ... an infrastructure for **mobile** and ..., 2002 - books.google.com

... that takes in open standards-based MPEG video and audio, provides **broadcast** service through real ... X. 509 v3 certificates and **public key**/private key encryption are used for further ... References
1. Pereira, JM; Fagen, D. Personal, Indoor and **Mobile Radio** Communications, 1996. ...

[Related articles](#)

... electronic digital rights management, secure transaction management and content ...

D Runje, M Kovac, BD Litman, J Orsulic, ... - US Patent App. 09/ ..., 2000 - Google Patents

... 18,2001 Sheet 41 of 48 US 2001/0032312 AI 0 181 **Public Key** Encrypt CONTENT_KEY with LMD Public Encryption Key Copy USAGE_RIGHTS from ... 186 187 **Decrypt CONTENT** KEY Store CONTENT_KEY and Usage Rights Delete Information About LICENSE REQ End ...

[All 3 versions](#)

Secure dynamic link allocation system for mobile data communication

DA Preston, RP Lutter, MA Benjamin, TJ ... - US Patent App. 09/ ..., 2001 - Google Patents
 ... Systems and methods are disclosed for layered, secure data communications with a **mobile** unit over a variety of different communication links, such as in-band signalling, SMS, CDPD etc. A privilege control table determines permitted classes of messages. **Content** labeling is ...
[All 5 versions](#)

Radio frequency identification (RFID) based network access management

H Waris - US Patent App. 10/610,974, 2003 - Google Patents
 ... for encrypted advertisements sent by the AP 70, which contain eg the **public key** required for ... could inform each other about websites in a timing-independent (asynchronous) **broadcast** by leaving ... link layer information and IP layer information for use by said **mobile** terminal for ...
[All 2 versions](#)

Method and system for delivering encrypted content with associated geographical- ...

MC Pelletier - US Patent App. 09/909,564, 2001 - Google Patents
 ... Advertisement is selected to be associated with the delivery of encrypted digital **content** if the address verification system returns an ... o _j O _J o 4 O) ; y - / HELPER I APPLICATION I WATER- I MARKING 1 SECURE CONTAINER PROCESSOR **DECRYPTION** RE- ENCRYPTION ...
[All 4 versions](#)

Method and system for securing local database file of local content stored on end- ...

RL Spagna, T Zhao, DR Geisler, JC ... - US Patent App. 09/ ..., 2001 - Google Patents
 ... Next, **decrypting** one or data items with the first **decrypting** key. Populating the data table with data items at locations specified in the reference table. 70? 130 100 **CONTENT** PROVIDER(S) (@\ PCM VS-V CM CO -*.- ^ PROCESSING TOOL WORKFLOW /- jet I ...
[All 4 versions](#)

Stop-and-go-MIXes providing probabilistic anonymity in an open system

D Kesdogan, J Egner, R Büschkes - Information Hiding, 1998 - Springer
 ... For special environments like eg **broadcast** networks superposed sending could be applied to reduce the cost (ie bandwidth). ... to equal length (agreement), combined with a secret random number (RN) and encrypted with the **public key** of the ... MIX 2 MIX 1 • **decrypt** • reorder •
[Cited by 168](#) - [Related articles](#) - [All 13 versions](#)

Proof of soundness (integrity) of cryptographic protocols

GJ Simmons - Journal of Cryptology, 1994 - Springer
 ... very natural rewrite rules of her program that the Simmons' selective **broadcast** key distribution ... concerned with the problem of providing for secure communications in a **mobile radio** network ... carry out the easy one of a complementary pair of **public key** (asymmetric) cryptographic ...
[Cited by 12](#) - [Related articles](#) - [BL Direct](#) - [All 2 versions](#)

[CITATION] Visual communications of tomorrow: natural, efficient, and flexible

J Konrad - IEEE Communications Magazine, 2001
[Cited by 24](#) - [Related articles](#) - [BL Direct](#) - [All 12 versions](#)

Method and apparatus for monitoring packet based communications in a mobile ...

DA Preston, RP Lutter - US Patent App. 09/841,755, 2001 - Google Patents
 ... For example, the VCOs 20 may constantly **broadcast** GPS data. The GPS service may currently bill each customer a particular fee per month. ... 24, 2002 the acknowledgement to make sure the **mobile** unit 10 used the correct **public key** for encrypting the COS data. ...
[All 4 versions](#)

[PDF] Applying digital watermarking techniques to online multimedia commerce

J Zhao - Proc. of the International Conference on Imaging ..., 1997 - CiteSeer
 ... image and the session key which is encrypted with the client's **public key**, to the ... A Java-based

mobile agent is under development to monitor and analyze images on the ... However, effective use in fields such as digital camera, DVD, digital **broadcasting**, electronic commerce, and ...

[Cited by 18](#) - [Related articles](#) - [View as HTML](#) - [All 13 versions](#)

[... , methods, and apparatus for unlocking value-added services on the **broadcast** ...](#)

WP Lord, AV Marolda, M Rosner - US Patent App. 09/970,756, 2001 - Google Patents

... manufacturer 32, vendor 10, or ad agency 12 is the provider of the **mobile** device 24 ... The signed hash, along with other information such as the hashing algorithm and the **public key** of the ... In step S106, the ad, hash, and certificate are **broadcast** by the broadcaster to the Receiver ...

[All 3 versions](#)

[CITATION] An embedded cryptosystem for digital broadcasting

GS Sundaram, S Sista - 1997 IEEE 6th International Conference on Universal ..., 1997

[Related articles](#)

Method and device for authorizing content operations

FLAJ Kamperman, GJ Schrijer - US Patent App. 10/531,939, 2003 - Google Patents

... In the **broadcast** world, systems of this category are generally known as conditional access (CA) systems, while in ... data or on the basis of an ID device (eg a wireless smart card, the **mobile** telephone, etc ... 0093] Suppose an ID device operates with some **public key** algorithm using ...

[All 4 versions](#)

A wireless-based authentication and anonymous channels for large scale area

WD Lin, JK Jan - iscc, 2001 - computer.org

... that supports location anonymity and MSs identity anonymity for roaming, dynamic channel assignment and **broadcasting**. ... In our method when **mobile** station M wants to send an anonymous message in ... messages, except HD and N 1 will be encrypted by H's **public key** for sake ...

[Cited by 21](#) - [Related articles](#) - [All 5 versions](#)

Secure broadcast/multicast service

P Ahonen, U Ilkka, M Vesa-Matti - US Patent App. 10/527,368, 2002 - Google Patents

... to listen to music and watch concerts and football games via their **mobile** handsets ... node sends the allocated Key Encryption Key to the user encrypted with that user's **public key**. ... a first, home communication network and wishes to participate in a multicast or **broadcast** service via ...

[All 5 versions](#)

[PDF] IP Multicast Push and Broadcast on Demand in FRA Networks

H Linder, W Stering, J Norbury - EMBRACE public deliverable D, 2002 - telenor.no

... 40 4.6.2. **Content** Encryption ... Virtual Circuit PVR Personal Video Recorder QoS Quality of Service QPSK Quadruple Phase Shift Keying RF **Radio** Frequency RRMP ... The concept of **Broadcast** on Demand (BoD) relies on the assumption that, in a BFWA operation where cell ...

[Cited by 2](#) - [Related articles](#) - [View as HTML](#)

New Technologies of Digital Watermarking for Digital Broadcasting System

CC Wang - 2003 - etd.ncku.lib.ncku.edu.tw

... connect user to Internet. Hence in addition to providing basic **radio** and TV broadcasts, ... TV Distribution Figure 1.5 Watermark detection points in **broadcasting** system. ... It can be seen that cryptography can protect **content** in transit, but once **decrypted**, the **content** has no further ...

[Cited by 1](#) - [Related articles](#) - [All 2 versions](#)

[... , wireless coverage and cooperation on data dissemination among **mobile** devices](#)

M Papadopoulou, H Schulzrinne - ... international symposium on **Mobile** ..., 2001 - portal.acm.org

... the source and the destina- tion are required to have PGP in order to encrypt (using the **public key**) and then ... with a constant speed uniformly selected from (0 m/s, 1.5 m/s). When a **mobile** host reaches ... The **broadcast** is scheduled at a random time selected from the on interval. ...

[Cited by 214](#) - [Related articles](#) - [All 34 versions](#)

System for distributing subscription and on-demand audio programming

N Schulhof, JM Janky - US Patent 5,572,442, 1996 - Google Patents

... may listen to recordings that they have purchased or recorded themselves when the program material was origi- nally **broadcast**, the **mobile** listener cannot ... However, the video-on-demand industry has a fundamentally different focus than that of **radio** or other audio-based ...

[Cited by 55](#) - [Related articles](#) - [All 2 versions](#)

[PDF] Public access mobility LAN: extending the wireless Internet into the LAN ...

J Li, SB Weinstein, J Zhang, N Tu - IEEE Wireless Communications, 2002 - cs.bilkent.edu.tr

... A VLAN is a logical grouping and **broadcast** containment mechanism in a switched LAN environment. ... The **public key** is used to securely inform the **mobile** user of the session key while all ... Since only an authenticated **mobile** device shares a session key with the access point and ...

[Cited by 16](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 7 versions](#)

Secure electronic **content** management system

E Downs, GG Gruse, MM Hurtado, C Medina, ... - US Patent ..., 2003 - Google Patents

... 1, 1986.* Quantum **Public Key** Distribution System, IBM Technical Disclosure Bulletin, Apr. ... Pedro R. Kanof (74) Attorney, Agent, or Firm—Steven J. Meyers; David M. Shofi; Fleit,Kain,Gibbons, Gutman & Bongini PL (57) ABSTRACT A method of managing **content** data and ...

[Cited by 7](#) - [Related articles](#) - [All 2 versions](#)

[PDF] Mutual Authentication in Wireless Networks

RR Joos, AR Tripathi - 1997 - Citeseer

... The next section will provide an elaboration of the protocol's short-comings for **mobile** environments ... initiates the protocol by requesting PB's key from S. This request is **broadcast** in clear ... now contacts PB directly by sending a nonce and PA's identity encrypted in PB's **public key**. ...

[Cited by 9](#) - [Related articles](#) - [View as HTML](#) - [All 3 versions](#)

[PDF] An infrastructure for **mobile** agents: requirements and architecture

A Lingnau, O Drobnik - Proceedings of the 13th DIS Workshop, 1995 - Citeseer

... communication schemes such as synchronous or asyn- chronous RPC, multicast or **broadcast** can be ... a trustworthy, disinterested third party which serve as a meeting place for **mobile** agents that ... knows about the servers in its vicinity, it is easy to support **public-key** encryption for ...

[Cited by 43](#) - [Related articles](#) - [View as HTML](#) - [All 4 versions](#)

[PDF] Security of **mobile** and wireless networks

KJ Grahm, G Pulkkis, JS Guillard - Information Science, 2002 - Citeseer

... Authentication for users passing between different networks will also be protected using a **public key** cryptographic system. ... **content** provision, wireless multimedia, multimedia **broadcast** information processing, information search ... Security of **Mobile** and Wireless Networks 598 ...

[Cited by 1](#) - [Related articles](#) - [View as HTML](#) - [All 7 versions](#)

Method and system for connecting a **mobile** terminal to a database

H Rautila, J Kil, K Ratschunas - US Patent 6,549,625, 2003 - Google Patents

... of transceivers without or in a local area network by a short range **radio** link having a ... location 16 or to generate the signal 39 to cause the error message to be **broadcast**. The **mobile** terminal 12 includes first and second trans- ceivers which respectively are a transceiver which is ...

[Cited by 4](#) - [Related articles](#) - [All 5 versions](#)

Go o o o o o o o o o g l e ►

Result Page: 1 2 3 4 5 6 7 8 **Next**

"public key" broadcast (mobile OR radio) decrypt content - Google Scholar

Search

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2010 Google